Leçon 2

La charte d'usage de l'internet

Objectifs

- Protéger la vie privée des internautes ;
- Sécuriser les données ;
- Se protéger contre les attaques de pirates.

Plan de la leçon

I. La protection de la vie privée

1. Définition
2. Les règles de prudence

II. La sécurité des données

1. Les risques des données
2. Les règles de prudence

Leçon 2 :

La charte d'usage de l'internet

I. La protection de la vie privée :

1. Définition

C'est l'ensemble des règles et des conventions qui déterminent les droits et les obligations de l'utilisateur face à l'usage de l'Internet.

2. Les règles de prudence

Activité 1 :

1) Est ce que vous pouvez consulter la boîte e-mail de votre ami ? Pourquoi ?
2) Si vous disposez par exemple des photos de votre ami, est ce que vous pouvez les envoyer à d'autres personnes ? Pourquoi ?
3) Est ce que vous pouvez mettre vos informations personnelles sur Internet ? Pourquoi ?

Constatation :

Pour pouvoir protéger votre vie privée sur Internet, vous devez :

- ✓ Garder votre mot de passe en secret
- ✓ Ne diffusez pas vos photos sur Internet
- ✓ Ne diffusez pas des informations personnelles sur Internet
- ✓ Soyer polis et courtois lorsque vous écrivez vos e-mails

II. La sécurité des données

La sécurité informatique, est l'ensemble des mesures prises pour protéger un ordinateur et les données qu'il contient contre les dangers et les risques de l'Internet.

Activité 2 :

1) Lorsque vous recevez un fichier joint, est ce que vous l'ouvrez directement ? pourquoi ?
2) Lorsque vous recevez un e-mail d'une personne inconnue, est ce que vous l'ouvrez ? Pourquoi ?
3) Lorsque vous vous connectez sur un site et vous apparaît un message « si vous cliquez vous gagnerez 1000 euro », est ce que vous acceptez ? pourquoi ?

1. Les risques de l'Internet

a) Les virus informatiques : Un virus informatique est un programme qui s'attaque aux ordinateurs pour modifier ou pour détruire les informations.

Les différents de virus sont :

- ✓ **Les vers (ou worms) :** C'est un type de virus particulier, il s'agit de programmes capables de se propager soit à travers le réseau local soit via Internet (qui provient généralement des e-mails), puis d'exécuter certaines actions pouvant porter atteinte à l'intégrité des systèmes d'exploitation.
- ✓ **Les chevaux de Troie (ou trojan) :** C'est un programme qui contient en réalité une fonction illicite cachée, permet la pénétration dans des fichiers pour les consulter, les modifier ou les détruire. A la différence d'un ver, le cheval de Troie ne se réplique pas.
- ✓ **Les keyloggers :** C'est un logiciel qui enregistre les frappes au clavier pour voler, par exemple, un mot de passe.
- ✓ **Les macrovirus** : Ils contaminent les fichiers bureautiques (traitement de texte, tableur, présentation multimédia).
- ✓ **les virus de boot (d'amorçage)** : résident dans le secteur de boot du disque dur. Il s'exécute lorsque votre ordinateur démarre. Ils sont très incrustés dans l'ordinateur et difficiles à éradiquer

b) Le piratage : Le piratage consiste à une intrusion réussite par une personne non autorisée à un ordinateur connecté à l'Internet, ce dernier peut modifier et supprimer les informations sur cet ordinateur.

2. Les règles de prudence technique

- ✓ Installez un antivirus et faire son mise à jour régulièrement.
- ✓ N'ouvrez pas les e-mails qui proviennent des personnes inconnues.
- ✓ N'ouvrez pas les disquettes, les CD ou bien les DVD sans les vérifier avec la dernière mise à jour de votre antivirus.
- ✓ Utiliser un firewall (un pare à feu) qui est un dispositif informatique qui permet d'éviter les accès non autorisés à partir de l'Internet.